Tabla de Contenido

1. OBJETO 2
2. ALCANCE DEL OBJETO 2
3. CONTEXTUALIZACIÓN 2
4. REQUERIMIENTOS GENERALES 3
5. ESPECIFICACIONES TECNICAS DE LOS COMPONENTES DE LA SOLUCION 4
5.1 Diseño de la solución requerida. 5
5.2 Requerimientos para la plataforma Hiperconvergente 5
5.3 Requerimientos Equipos de Red (Switches de Core de Datacenter) 11
5.4 Requerimientos Firewalls de Nueva Generación 14
5.5 Requerimientos Firewall de aplicaciones y Balanceador de cargas 29
6. MANTENIMIENTO PREVENTIVO Y CORRECTIVO 34
7. SOPORTE TÉCNICO 35
6.1 Procedimiento de reporte de casos de soporte 36
8. ACUERDOS DE NIVELES DE SERVICIOS 36
9. EQUIPO DE TRABAJO MÍNIMO REQUERIDO 37

1. OBJETO

Contratar la adquisición de infraestructura tecnológica de seguridad y de servidores para la Sociedad de Activos Especiales S.A.

2. ALCANCE DEL OBJETO

La adquisición de infraestructura tecnológica surge de la necesidad de renovación de la plataforma tecnológica que permita a la SAE soportar de forma óptima los procesos de negocio. La adquisición de infraestructura tecnológica incluye:

a. Entrega, instalación y configuración de plataforma hiperconvergente de servidores con mínimo tres años de garantía y soporte técnico.
b. Migración de infraestructura de servidores actuales a la plataforma hiperconvergente adquirida y configuración de integración con la plataforma de nube publica de la entidad.
c. Entrega, instalación y configuración de equipos de gestión unificada de amenazas (UTM) con mínimo tres años de garantía y soporte técnico.
d. Entrega, instalación y configuración de switches de core de servidores con mínimo tres años de garantía y soporte técnico.
e. Entrega, instalación y configuración de firewall de aplicaciones (WAF) y balanceador de cargas con mínimo tres años de garantía y soporte técnico.
f. Transferencia de conocimiento certificada en la administración de todos los componentes adquiridos.

3. CONTEXTUALIZACIÓN

La Sociedad de Activos Especiales tiene su plataforma de cómputo en modalidad de collocation con acceso de sus usuarios mediante canales MPLS (para sus 6 sedes a nivel nacional) o Internet.

La plataforma de servidores se encuentra virtualizada con Microsoft Hiper-V 2012 R2 teniendo como base sistema operativo Windows Server 2012 R2 Datacenter licenciado por CPU, esta plataforma soporta 67 servidores virtuales, con la siguiente distribución de sistemas operativos:

Sistema Operativo	Versión	Cantidad
Microsoft Windows	2012 R2 Datacenter	50
Microsoft Windows	2016 Standard*	5
CentOS	6.5	2

CentOS	7.1	1
CentOS	7.4	6
Debian	7.4	2

* Windows server 2016 se encuentra licenciado de forma independiente por core asignado a los servidores virtuales.

De la plataforma de servidores mencionada, aproximadamente el 50% pertenece a servidores que se deberán soportar sobre la plataforma hiperconvergente, por lo que se requiere su migración desde la infraestructura actual.

Por otra parte, a nivel de seguridad, la entidad cuenta con firewalls Fortinet configurados en alta disponibilidad con funcionalidades de Control de aplicaciones, Proxy transparente, filtro de contenido web, IPS, IDS, VPN SSL, VPN Site to Site, DDoS, Traffic Shapper, Routing, entre otras.

4. REQUERIMIENTOS GENERALES

a. Entregar, instalar y configurar todos los componentes requeridos para que los equipos a entregar (servidores, equipos UTM, switches, WAF, balanceador) se conecten de forma óptima entre ellos y con los demás equipos de infraestructura de la Entidad. Todas las conexiones de red entre los componentes deben realizarse a 10Gbps mediante fibra óptica, centralizándose en los switches de Core de Datacenter a entregar por parte del proveedor.
b. Todos los componentes (hardware y software) a entregar deben contar con garantía directa de fabrica cómo mínimo de tres (3) años.
c. Realizar cómo mínimo un mantenimiento preventivo por cada año de soporte y garantía entregados, realizando actualización de firmware, de software y realizando las reconfiguraciones derivadas de nuevas versiones de software o firmware instalados.
d. El proveedor deberá entregar el licenciamiento requerido para cumplir cualquier requerimiento técnico que se establece en este documento, en cualquiera de los componentes solicitados, dicho licenciamiento deberá alinearse con la garantía general solicitada para los diferentes componentes e ingresar al esquema de soporte prestado para el componente al que pertenece (renovación de soporte, ANS para soporte, etc).
e. Se debe configurar cualquiera de las opciones y capacidades requeridas en este documento en la fase de instalación y configuración o durante la fase de soporte de la infraestructura entregada. Al igual que cualquiera opción por defecto que incluya el fabricante de la plataforma y que la entidad decida implementar.
f. Todo el hardware o software objeto de esta contratación debe ser funcional tanto en los protocolos IPv4 e IPv6. Se debe tener un similar comportamiento y se debe proporcionar para ambos protocolos de entrada, salida y/o el rendimiento de flujo de datos, así como rendimiento en la transmisión y el procesamiento de paquetes.

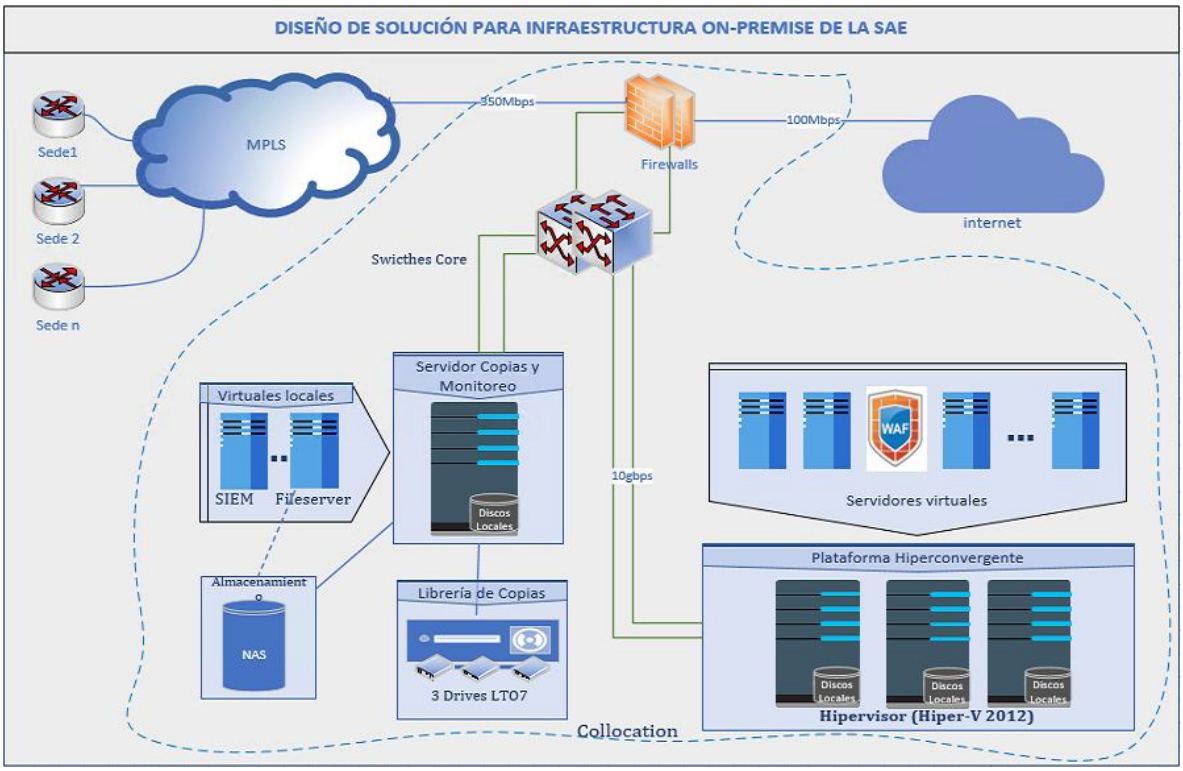
g. El proveedor debe certificar mediante una declaración de competencias técnicas en IPv6 de parte del suministrador o integrador del equipamiento. Se requiere conocimiento y experiencia en IPv6 como forma de asegurar una apropiada instalación e integración de IPv6 en ambientes de las TIC.
   La declaración debe indicar bajo juramento de ley:
   - Que tienen suficiente número de empleados para cumplir con los servicios ofertados.
   - Que estos empleados han sido entrenados profesionalmente para su trabajo de diseño, integración y/o construcción de equipamiento de las TIC en ambientes IPv4 e IPv6
   - Que la calidad de los servicios ofertados cumple todos los requerimientos definidos en los documentos de la contratación y que estos requerimientos aplican tanto para IPv4 como para IPv6.

h. El soporte de IPv6 debe ser certificado por el IPv6 Ready Logo. El equipo que no se encuentre habilitado a través de los procedimientos de pruebas IPv6 Ready debe cumplir con las RFC que se listan en el Anexo N 2. del presente documento "RFC a validar en hardware y software a adquirir"

5. ESPECIFICACIONES TÉCNICAS DE LOS COMPONENTES DE LA SOLUCIÓN

A continuación, se establecen los requerimientos y especificaciones técnicas que deben cumplir cada uno de los componentes a entregar. Todos los requerimientos a continuación listados se deben incluir en los costos de las soluciones, la entidad podrá solicitar la configuración y puesta operación de cualquier funcionalidad o requerimiento sin que implique costo adicional.

5.1 Diseño de la solución requerida.



5.2 Requerimientos para la plataforma Hiperconvergente

SOLUCION OFRECIDA:_____

CARACTERÍSTICA	REQUERIMIENTO TÉNICO MÍNIMO	CUMPLIMIENTO (indicar capacidades o características si aplican)
1. Generalidades	a. La solución de hiperconvergencia deberá proveer un crecimiento modular y escalable, garantizando el aprovisionamiento tanto de cómputo, memoria y almacenamiento. b. El clúster de hiperconvergencia deberá incluir el licenciamiento de hipervisor con soporte mínimo por 3 años, sin costos adicionales para la entidad. c. La solución debe ser configurada con hipervisor Microsoft Hyper-V Server (2012 R2, 2016 o 2019) y debe integrarse con la plataforma de nube publica de Microsoft Azure, para lo cual se debe incluir el software (con su respectivo licenciamiento) y configuraciones necesarias para que la entidad pueda mover servidores virtuales entre las dos	

CARACTERÍSTICA	REQUERIMIENTO TÉNICO MÍNIMO	CUMPLIMIENTO (indicar capacidades o características si aplican)
	plataformas. El proveedor debe garantizar la gestión completa de las funciones de virtualización desde la plataforma hiperconvergente, integrándose con el software de gestión de virtualización de microsoft. d. El sistema debe incluir una funcionalidad que notifique automáticamente al fabricante acerca de condiciones de error de manera proactiva. e. El fabricante de la solución ofertada deberá estar calificado como líder en el cuadrante mágico de Gartner más reciente para infraestructura hiperconvergente. f. El fabricante de la solución debe certificar que la solución que se entregará a la SAE está validada directamente por él, mediante carta dirigida a la entidad, firmada por el representante legal o la persona competentemente delegada para ello. Esta validación se debe realizar nuevamente cuando la solución sea puesta en operación en la Entidad. g. El proveedor deberá entregar los catálogos y links de verificación de cumplimiento de los requerimientos técnicos para la solución ofrecida. Los cuales deben ser verificables en la página del fabricante de la solución. h. La plataforma hiperconvergente deberá tener un único punto de soporte de hardware y software. i. Se debe permitir configurar varias redes (VLANs) en la solución, de forma que se puedan segmentar la redes entre los servidores virtuales.	
2. Hardware	La solución de hiperconvergencia deberá incluir mínimo 3 nodos en clúster garantizando las siguientes características: a. Cada nodo deberá incluir mínimo dos (2) procesadores de la familia Intel Skylake Gold o superior con 16 Cores por CPU como mínimo, de la última generación liberada por el fabricante. Los nodos de hiperconvergencia ofertados deberán garantizar como mínimo 108 cores físicos en el clúster. b. La solución debe garantizar como mínimo 47 TB efectivos sin compresión ni deduplicación o algoritmos de optimización, con factor de replicación mínimo de 2, en almacenamiento híbrido con discos SSD (estado sólido) y HDD (rotacionales o mecánicos). Para el caso de ofrecer discos HDD de 7.200 RPM, la capacidad neta de éstos no debe superar el 76% del almacenamiento neto ofrecido con la combinación de los dos tipos de discos. c. El proveedor deberá estimar y entregar el almacenamiento necesario para garantizar que, en caso de falla o indisponibilidad de uno de los nodos del clúster, el porcentaje de uso del almacenamiento en los dos nodos restantes no superará el 85% de la capacidad neta requerida (47 TB).	

CARACTERÍSTICA	REQUERIMIENTO TÉNICO MÍNIMO	CUMPLIMIENTO (indicar capacidades o características si aplican)
	d. De igual forma se debe estimar el almacenamiento necesario a entregar para que el porcentaje de uso en operación normal de los tres nodos no supere el 75% respecto a la capacidad neta requerida (47 TB). Esto significa que el proveedor deberá entregar un almacenamiento mínimo neto (efectivo) utilizable por la Entidad de 63TB (TeraBytes) sin que este valor se estime a partir de logros de deduplicación o compresión de los datos, con un factor de replicación de los datos de mínimo 2 (RF2), sin superar el limite de porcentaje máximo de almacenamiento ofrecido con discos mecánicos de 7200rpm, establecido en el punto anterior. e. El clúster de hiperconvergencia ofertado, como mínimo deberá garantizar 1536 GB de memoria RAM efectivos, DDR4 o superior, dejando capacidad de crecimiento cómo mínimo del 30% de la capacidad inicial requerida, sin que se requiera combinar capacidades de DIMMS o cambiar DIMMS entregados inicialmente. f. Cada nodo debe tener mínimo dos (2) Puertos 10GB SFP+ o los necesarios para la interconexión de los nodos ofertados a un mínimo de 20GB entre ellos, con los conectores (transceivers SFP+) y cables de conexión respectivos. g. Cada nodo deberá contar con mínimo dos (2) puertos adicionales Ethernet 10G RJ45 o SFP+ para tráfico de administración, Backup, replicación, entre otros. En caso contrario la capacidad de conexión a la red deberá ser mínimo de 10GB adicionales (por nodos) a los requeridos en el numeral anterior. h. La solución de hiperconvergencia debe configurarse en IPV4 e IPV6. i. Cada nodo debe tener dos (2) fuentes de alimentación AC, Voltaje 200 to 240 VAC, frecuencia 50/60 Hz, deberá soportar la inserción y remoción en caliente (Hot-Swap) j. Todas las tecnologías de Alta Disponibilidad (HA) deben funcionar tal como fueron diseñadas aún con clúster heterogéneos. k. Cada nodo ofertado debe tener un máximo de dos (2) unidades de RACK. l. El proveedor deberá incluir los cables (eléctricos, red, fibra óptica, entre otros) y rieles de montaje. m. La solución podrá incluir switches de comunicación (máximo 2 switches con 1U de Rack cada uno), los cuales serán considerados parte de la solución hiperconvergente y por lo tanto se debe incluir el licenciamiento requerido para su operación e integración con los nodos hiperconvergentes, al igual que los esquemas de soporte y garantía, y cualquier otro requerimiento técnico que aplique a la solución hiperconvergente.	

CARACTERÍSTICA	REQUERIMIENTO TÉNICO MÍNIMO	CUMPLIMIENTO (indicar capacidades o características si aplican)
3. Crecimiento	a. Mostrar alertas cuando el uso de los recursos de memoria o almacenamiento exceda el límite para soportar la indisponibilidad de uno de los nodos de cómputo. b. La solución deberá admitir la escalabilidad de nodos dentro del mismo clúster. Una vez un nuevo nodo sea instalado en el clúster, el sistema debe balancearse de manera automática.	
4. Compresión y deduplicación	a. El sistema hiperconvergente debe llevar a cabo las tareas de compresión y deduplicación completamente en software sin requerir el uso de ninguna conexión directa entre nodos ni dispositivo de hardware especializado para esta labor. b. La solución debe poder ejecutar deduplicación y compresión a lo largo de todo el clúster (de forma global) y no limitadas al contenido de los discos de cada nodo.	
5. Almacenamiento	a. La solución debe permitir crear discos virtuales cuya única limitación de tamaño sea el espacio disponible en el clúster conservando la protección de los datos en caso de falla de alguno de los nodos o discos físicos en los que se alojan los datos del disco virtual. b. La solución deberá contar con una capa de caché distribuido en todos los nodos del clúster basada en discos SSD, con el objetivo de acelerar las peticiones de escritura y lectura c. El sistema debe hacer uso de una porción de la memoria RAM asignada como cache de lectura	
6. Disponibilidad	a. La solución debe soportar Windows Guest Failover Clúster, funcionalidad que permite alta disponibilidad para las aplicaciones configuradas en clúster en una VM (Con sistema operativo Windows Server 2012 R2 o Windows Server 2016) para que transparentemente realice el failover hacia otra VM ubicada en el mismo o en diferente host. b. La solución debe distribuir los datos en el almacenamiento interno del clúster y adicionalmente replicarlos internamente para poder asegurar su disponibilidad, basados en Software. c. Todos los componentes físicos que hagan parte de la solución y que realicen tareas de conexiones entre los nodos, deben contar con alta disponibilidad, con el fin de mitigar riesgos de indisponibilidad ante la falla de un componente físico. d. La solución debe detectar de manera proactiva el daño de un disco, removerlo automáticamente del clúster y reconstruir de manera inmediata los datos que ahí se alojaban en los otros discos del clúster. En caso de que el disco sea removido o haya estado fuera de línea	

CARACTERÍSTICA	REQUERIMIENTO TÉNICO MÍNIMO	CUMPLIMIENTO (indicar capacidades o características si aplican)
	(offline), la reconstrucción de los datos también debe iniciarse de manera automática e inmediata. e. La solución debe incluir la funcionalidad de replicación asincrónica de datos que cumpla con los siguientes requerimientos básicos: - Replica a nivel de máquina virtual de forma granular. - Mecanismos de compresión y de-duplicación de los datos a ser replicados. f. El sistema debe ofrecer la capacidad de mantener consistente la replicación de un grupo de volúmenes y/o máquinas virtuales de tal manera que los snapshot se tomen en el mismo punto en el tiempo. La detención de la réplica de uno de los volúmenes o VMs en el grupo de consistencia debe detener la réplica de todo el grupo. g. El sistema debe proveer la capacidad de programar la toma periódica de snapshots a máquinas virtuales, sin depender de funcionalidades heredadas del hipervisor. h. La solución debe incluir una arquitectura que provea a nivel de hardware y software un esquema de alta disponibilidad de tal forma que, ante la falla de un nodo, se mantenga operativo el clúster sin afectar el desempeño de las aplicaciones. i. La plataforma debe quedar instalada de forma que un nodo pueda entrar en modo mantenimiento, preservando la disponibilidad de los datos y asegurando la redundancia configurada para los datos desde el mismo momento en que el nodo queda en modo mantenimiento.	
7. Monitoreo y administración	a. La solución propuesta debe incorporar la capa de software de gestión de la infraestructura de hiperconvergencia instalada como un servicio en cada uno de los nodos que componen la solución manteniendo una arquitectura de alta disponibilidad, garantizando la consistencia y disponibilidad de la información. b. La solución deberá ofrecer un único dashboard para gestionar y aprovisionar máquinas virtuales, red, almacenamiento, controlar el rendimiento y gestionar eventos y alertas. c. La solución debe proveer información de monitoreo a lo largo del tiempo y presentar proyecciones de uso o agotamiento de recursos de acuerdo con el histórico de monitoreo. d. Adicionalmente debe permitir entregar estadísticas completas sobre las máquinas virtuales como consumos de vCPU, RAM, y discos, así como IOPS, working set de lectura, working set de escritura y latencias. e. La solución debe entregar el detalle a nivel de disco virtual, como mínimo las siguientes estadísticas: Latencias de escritura y lectura, IOPS de escritura y lectura, cantidad de datos leídos de cache, cantidad de	

CARACTERÍSTICA	REQUERIMIENTO TÉNICO MÍNIMO	CUMPLIMIENTO (indicar capacidades o características si aplican)
	datos leídos de SSD, cantidad de datos leídos de HDD, cantidad de datos activos (Working Set) y el porcentaje de I/O aleatorio (no secuencial) f. La solución debe permitir el análisis de ancho de banda utilizado por la misma, así como el ancho de banda de una máquina virtual. g. La interface gráfica de administración debe ser accedida mediante un browser basado en web. No se aceptarán soluciones que ofrezcan consolas de gestión externas o mediante software de gestión adicional. h. La solución debe proveer accesos alternativos basados en SSH y/o interfaces seriales remotas estilo IPMI. i. La interface gráfica de administración debe soportar autenticación LDAP Active Directory. j. La solución deberá proporcionar un mecanismo de actualización del software de la infraestructura completa del clúster (servicios de storage, firmware de los nodos e hipervisor) directamente desde la consola web y de forma no disruptiva, es decir, sin necesidad de reinicio de las máquinas virtuales ni indisponibilidad del servicio. k. La solución debe soportar integración mediante el uso de REST API a otras soluciones de administración para facilitar la integración con ambientes de monitoreo actuales. l. No debe haber puntos únicos de falla en la capa de administración de la solución, todos los nodos en el sistema deben tener un módulo de software nativo en el sistema hiperconvergente que permita hacer la administración centralizada de todo el clúster o clúster´s de la solución. Esta funcionalidad no debe implicar configuraciones adicionales a la del sistema m. El proponente deberá entregar la documentación de la definición, diseño y planeación de Arquitectura para la solución ofertada.	
8. Entrega, Instalación configuración y migración	a. El proveedor deberá entregar el hardware y software completo la solución en un tiempo máximo de 45 días calendario b. El proveedor deberá realizar la configuración de la solución para que soporte los servidores virtuales, servicios de aplicaciones, firewall de aplicaciones y balanceador en modo dual stack (IPv4 e IPv6). c. El proveedor deberá realizar la migración de todos los servidores virtuales hacia la nueva infraestructura verificando en conjunto con los administradores de la entidad que los servicios de cada uno de éstos queden operando de forma correcta en modo dual stack (IPv4 e IPv6). d. Entregar documento que acredite titularidad y vigencia de la totalidad del licenciamiento requerido para la solución de hiperconvergencia, a nombre de la Sociedad de Activos Especiales	

CARACTERÍSTICA	REQUERIMIENTO TÉNICO MÍNIMO	CUMPLIMIENTO (indicar capacidades o características si aplican)
	e. La instalación, configuración y puesta en marcha de la solución de Hiperconvergencia debe incluir transferencia de conocimiento y capacitación necesaria para la administración de la totalidad de herramientas y componentes que integran la solución de hiperconvergencia en un plazo máximo de 30 días calendario f. Todos los componentes de la solución deben ser instalados, conectados, configurados e integrados con los demás componentes de la infraestructura tecnológica de la entidad, tanto los existentes como los componentes que hacen parte del presente proceso (Switches core, firewalls, WAF, balanceadores, etc). g. Los servicios de instalación, configuración y puesta en operación de la solución de hiperconvergencia ofertados deben ser realizados por el contratista; con personal certificado por el fabricante, idóneo y experto en soluciones ofertadas a la entidad. h. El traslado, instalación, gastos administrativos, y demás gastos y servicios adicionales que se requieran para garantizar el óptimo funcionamiento de la solución de hiperconvergencia no debe representar costos adicionales para la Entidad.	
9. Certificados de fabricante	a. El proveedor debe ser canal (partner) certificado por el fabricante de la solución ofertada y estar en capacidad técnica de configurar, mantener y dar soporte técnico de los equipos. En consecuencia, el oferente deberá presentar la certificación correspondiente, la cual deberá ser verificable en medios dispuestos por el fabricante. El documento entregado debe ser expedido por el fabricante de los equipos ofertados con fecha no mayor a 30 días dirigido a la Sociedad de Activos Especiales.	

5.3 Requerimientos Equipos de Red (Switches de Core de Datacenter)

EQUIPOS OFRECIDOS:_____

CARACTERÍSTICA	REQUERIMIENTO TÉNICO MÍNIMO	CUMPLIMIENTO (indicar capacidades o características si aplican)
1. Puertos	a. 24 puertos de 10GBASE-X SFP+ (1Gb/10Gb velocidad dual) b. Un Puerto Serial RJ-45 para control c. Un puerto 10/100/1000BASE-T para administración.	

<table>
<tr><td></td><td>d. Los puertos requeridos para realizar la configuración en stack entre lo switches de core con un mínimo de 40Gbps, y para realizar la conexión entre switches que puedan hacer parte de la plataforma hiperconvergente con un mínimo de 20Gbps por switch.</td><td></td></tr>
<tr><td>2. Tranceivers</td><td>a. El proveedor deberá entregar la cantidad de puertos, transceivers y cables necesarios para conectar la solución hiperconvernegente a los switches de red a proveer, con un número mínimo de 2 conexiones a 10Gbps con fibra óptica por switch.

b. Adicionalmente, para las conexiones de los demás componentes de la entidad de entregar los siguientes conectores y cableado para ambos switches:
<table>
<tr><th>Cantidad</th><th>Descripción</th></tr>
<tr><td>8</td><td>10 Gigabit Ethernet SFP+ module, 850nm, MMF 26-300m link, LC connector</td></tr>
<tr><td>4</td><td>10Gb SFP+, 10GBASE-T RJ45, 30m with Cat6a
Nota: En caso de que el swicth no cumpla este requerimiento, el proveedor podrá entregar a la entidad 1 tarjeta dualport de red con puertos 10GB SFP+ para servidor dell R740, con los transceivers correspondientes a nivel de swicthes de core y a nivel de servidor. Se establece esta opción dado que la unidad debe conectar el servidor mencionado a la red a una velocidad de 10Gbps, el cual cuenta actualmente con conexiones 10GBASE-T RJ45.</td></tr>
<tr><td>24</td><td>1000BASE-T, RJ45 MINI GBIC</td></tr>
<tr><td>6</td><td>10 Gigabit Ethernet SFP+ passive cable assembly, 5m length.</td></tr>
<tr><td>4</td><td>Patchcord de fibra de 10Gb conector LC-LC de 3 Metros</td></tr>
<tr><td>2</td><td>Patchcords UTP RJ-45 Categoría 6a de 3 Metros</td></tr>
</table></td><td></td></tr>
<tr><td>3. Generalidades</td><td>a. Los equipos deben ser de máximo una unidad de rack (1U)
b. Tener fuente de poder redundante y ventiladores redundantes
c. Las fuentes de poder deben ser intercambiables en caliente
d. Los ventiladores se deben poder intercambiar en caliente
e. Deben permitir administración a través de línea de comandos y en modo gráfico. Administración vía SSH, SNMP (V1, V2 y V3)
f. Soportar SDN, OpenFlow, NetFlow o Sflow o Flexible Netflow o Netflow Lite
g. Deben permitir configurar ACLs (de nivel 2,3,4)
h. Debe soportar IGMP v3 snooping
i. Los equipos deben ser para montaje en Rack de servidores estándar de 19" de ancho.
j. Los equipos deben operar con energía eléctrica de 100 – 240V y frecuencia de 50 - 60 Hz.</td><td></td></tr>
</table>

4. Rendimiento	a. Capacidad de conmutación de paquetes mínima de 880 Gbps b. 2.4GHz Quad core CPU c. 4GB DDR3 ECC memory d. 32GB SSD memory	
5. Calidad de servicio	a. Deben soportar y estar incluido los siguientes estándares: • QoS—egress port rate shaping/limiting • IPv4 o Fast-direct broadcast o Ignore broadcast • IPv6 netTools—Ping, traceroute, BOOTP relay, DHCP, DNS, and SNTP.	
6. Apilamiento	a. Los equipos deben comportarse como una única entidad, administrable con una única dirección IP, con capacidad de trabajar en modo Activo-Activo. b. Los equipos deben soportar como mínimo 40Gb de velocidad de conexión de stack.	
7. Alta Disponibilidad	a. Los equipos deben estar configurados en alta disponibilidad integrando o soportando por cada equipo como mínimo: • Dos fuentes de poder AC. • Cuatro ventiladores	
8. Implementación	b. Los equipos deben ser configurados para soportar la operación a nivel de red de la Entidad, configurando las VLANs, Redes, ACLs, Enrutamiento que la entidad defina para la implementación óptima de los equipos y su interacción con los demás componentes de la infraestructura. Todas estas configuraciones se deben realizar tanto para IPv4 como para IPv6, garantizando el funcionamiento en modo dual-stack de la red de la Entidad. c. La instalación, configuración y puesta en marcha de los equipos debe incluir transferencia de conocimiento y capacitación necesaria para la administración de la totalidad de las funcionalidades del equipo entregado. La capacitación debe ser certificada directamente por el fabricante.	
9. Certificados de fabricante	a. El oferente debe ser canal (partner) certificado en mínimo nivel Oro del fabricante de los equipos ofertados y estar en capacidad técnica de configurar, mantener y dar soporte técnico de los equipos. Para esto, el oferente deberá presentar la certificación que lo acredite como partner de la marca ofrecida. Este documento debe ser expedido por el fabricante de los equipos ofertados con fecha no mayor a 30 días dirigido a la Sociedad de Activos Especiales. b. El oferente deberá presentar una certificación emitida por fabricante donde conste que los equipos entregados tienen soporte de fabrica por 3 años y que los mismos están en línea de producción	

	vigente. Este documento debe ser expedido por el fabricante de los equipos ofertados con fecha no mayor a 30 días, dirigido a la SAE.	
10. Documentación	a. El proveedor deberá entregar a la entidad • Manuales del fabricante del producto propuesto. • Documentación as built, que registre el estado de configuración e implementación al momento de la recepción formal de la solución (Informe definitivo de la Implementación) • Diagramas y planos. • Documentos de garantía • Manuales de administración. • Manuales de operación. • Manuales de usuario. • Documentación de licenciamiento. • Catálogos de la herramienta ofrecida. b. Es obligatorio, para el cumplimiento del requisito habilitante, incluir en su propuesta el catálogo o documentación técnica del fabricante, en el cual se permita la comprobación de lo ofrecido, se debe diligenciar este anexo indicando el número de folio y resaltar el párrafo en los catálogos donde se cumple con las características ofrecidas.	

5.4 Requerimientos Firewalls de Nueva Generación

EQUIPOS OFRECIDOS:_____

Se deberán ofrecer, configurar y poner en operación las funcionalidades que se detallan en la siguiente tabla

CARACTERÍSTICA	REQUERIMIENTO TÉNICO MÍNIMO	CUMPLIMIENTO (indicar capacidades o características si aplican)
1. Generalidades	a. Los equipos deben ser de arquitectura integrada de propósito específico para ofrecer un alto rendimiento y baja latencia.	

	b. Los equipos deben integrarse de forma nativa (fábrica) con el appliance virtual de monitoreo y correlación de eventos con el que cuenta la entidad (FortiSIEM). c. Los equipos deben soportar prevención de intrusos basada en anomalías, desfragmentación de paquetes y descarga de checksum. d. Los equipos deben soportar VPN, CAPWAP, aceleración de túneles IP, traffic shapping y prioridad de colas. e. Los equipos deben incluir aceleración de inspección de contenido basada en firmas, tráfico cifrado y texto claro. f. El fabricante de la solución debe estar validado a nivel de rendimiento y seguridad por los siguientes laboratorios de pruebas de terceros, líderes en la industria de protección: NSS Labs, VB100, AV Comparatives e ICSA. g. Los equipos deben contar con soporte técnico y retorno de hardware por parte del fabricante por un periodo de 3 años en un esquema 7 x 24 incluyendo actualizaciones de firmware, acceso al portal de soporte y recursos técnicos asociados. Los incidentes técnicos podrán ser reportados vía web, chat y teléfono. h. Los equipos deben debe proporcionar información granular para aplicaciones basadas en nube, tales como: YouTube, Dropbox, Baidu, Microsoft Office 365, Amazon, entre otras. i. Los equipos deben tener una base de datos que contenga una lista de direcciones Botnet C&C que sean actualizadas dinámicamente y almacenadas en el NGFW. a. El dispositivo debe permitir la definición de archivos por tipo o patrón de nombre a inspeccionar por el equipo dedicado para amenazas o malware avanzado. j. El dispositivo debe realizar balanceo de carga de enlaces estático mediante el uso de los siguientes algoritmos de balanceo de carga: o Ancho de banda: Asignar un peso a cada interfaz basado en la cantidad de paquetes. o Sesiones: Asignar un peso a cada interfaz basado en número de sesiones conectadas. o Spillover: Asignar un umbral a una interfaz para que cuando se exceda el tráfico sea enviado por otra interfaz. o IP fuente – destino: División de tráfico entre las interfaces por combinaciones de conexión entre direcciones IP fuente y destino. o IP fuente: División de tráfico por IP fuente.	

2. Rendimiento	a. El equipo deberá cumplir con las siguientes características mínimas de desempeño ya activas y funcionales: • Rendimiento de Firewall: 36 Gbps • Rendimiento de IPS: 10 Gpps • Rendimiento Inspección SSL: 8 Gbps • Rendimiento VPN IPSec: 20 Gbps • Rendimiento de NGFW: 9.5 Gbps • Rendimiento de protección de amenazas: 7 Gbps • Soporte de 8.000.000 sesiones concurrentes • Soporte de 10.000 políticas • Soporte a 10.000 usuarios VPN SSL • Almacenamiento incorporado: 2 discos SSD de 240 GB cada uno. • Doble fuente de poder	
3. Conectividad	a. El equipo deberá contar con las siguientes interfaces de conexión, completamente aprovisionadas: • 8 interfaces de 1Gbps RJ45 • 2 Puertos dedicados para administración • 8 Puertos GE SFP • 2 Puertos 10GE SFP+ • Puerto USB • 1 puerto de consola	
4. Traducción	a. NAT dinámico: Overloading y overlapping NAT b. NAT estático c. PAT d. NAT64, NAT46, NAT 66	
5. Funciones básicas de Firewall	a. Las reglas de firewall deben analizar las conexiones que atraviesen en el equipo, entre interfaces, grupos de interfaces (o Zonas) y VLANs. b. La solución debe configurarse en políticas basadas en identidad. Esto significa que podrán definirse políticas de seguridad de acuerdo con el grupo de pertenencia de los usuarios. c. La solución debe configurarse por políticas basadas en dispositivo. Esto significa que podrán definirse políticas de seguridad de acuerdo con el dispositivo (móvil, laptop) que tenga el usuario. Esta característica no debe requerir ningún tipo de licenciamiento adicional. d. Para los casos en los que la Entidad lo indique, se deben implementar las políticas basados en usuarios, grupos de	

	usuarios y dispositivos sobre una misma política, de esta forma se es lo más granular posible en la definición de políticas. e. El equipo deberá poder contar con la característica de modo de aprendizaje para políticas de firewall, cuyo objetivo sea monitorear el tráfico para determinar cuáles restricciones y protecciones se deben aplicar. f. Debe soportar la capacidad de definir nuevos servicios TCP y UDP que no estén contemplados en los predefinidos. g. Se deberán soportar y configurar reglas de firewall en IPv6 configurables tanto por CLI (Command Line Interface, Interface de línea de comando) como por GUI (Graphical User Interface, Interface Gráfica de Usuario). h. Se deben crear e integrar políticas contra ataques DoS las cuales se deben poder aplicar por interfaces. i. El dispositivo debe ejecutar inspección de tráfico SSL en todos los puertos y seleccionar bajo que certificado será válido dicho tráfico. j. Debe tener la capacidad de hacer escaneo a profundidad de tráfico tipo SSH dentro de todos o cierto rango de puertos configurados para dicho análisis.	
6. Conectividad y Enrutamiento	a. Funcionalidad de DHCP: como Cliente DHCP, Servidor DHCP y reenvío (Relay) de solicitudes DHCP. b. Soporte a etiquetas de VLAN (802.1q) y creación de zonas de seguridad en base a VLANs. c. Soporte de ruteo estático, incluyendo prioridades y/o distancias y/o prioridades de rutas estáticas. d. Soporte de enrutamiento basado en políticas para envió de tráfico de diferentes tipos basado en protocolo de tráfico entrante, dirección o interfaz fuente, dirección destino o número de puerto. e. Soporte a ruteo dinámico RIP, RIPNG, OSPF, OSPF6, BGP, IS-IS f. Soporte de ECMP (Equal Cost Multi-Path) g. Soporte a ruteo de multicast PIM SM y PIM DM. h. Soporte de reverse path lookup o anti-spoofing. i. Soporte de rutas blackhole. j. La solución permitirá la integración con analizadores de tráfico mediante el protocolo sFlow o Netflow. k. La solución podrá habilitar políticas de ruteo en IPv6 l. La solución deberá ser capaz de habilitar ruteo estático para cada interfaz en IPv6. m. Se deberán configurar las características de conectividad y enrutamiento que la unidad indique durante la fase de implementación y soporte a los equipos.	

7. VPN IPSEC	El equipo deberá soportar las siguientes características: a. Soporte a certificados RSA X.509 para construcción de VPNs cliente a sitio (client-to-site). b. Soporte de VPNs IPSec sitio a sitio y cliente – sitio. c. Soporte para IKEv2 e IKE Configuration Method d. Soporte de VPNs con algoritmos de cifrado: AES256, AES192, AES128, DES, 3DES e. Se debe soportar al menos el grupo de Diffie-Hellman 14. f. Se debe soportar los siguientes algoritmos de integridad: MD5, SHA-1 y SHA256. g. La VPN IPSec deberá poder ser configurada en modo interface (interface-mode VPN) h. Se deben soportar VPNs basadas en rutas y VPNs basadas en políticas. i. En modo interface, la VPN IPSec deberá poder tener asignada una dirección IP, tener rutas asignadas para ser encaminadas por esta interface y deberá ser capaz de estar presente como interface fuente o destino en políticas de firewall.	
8. VPN SSL	a. Capacidad de realizar SSL VPNs sin necesidad de licenciamiento por usuarios. b. Soporte a SSL 3.0, TLS 1.1 y 1.2 c. Soporte para modo de operación basado en web o modo túnel. d. Soporte a certificados RSA X.509 para construcción de VPNs SSL. e. Soporte de autenticación de dos factores. En este modo, el usuario deberá presentar un certificado digital además de una contraseña para lograr acceso al portal de VPN. f. Soporte de autenticación de dos factores con token, la solución debe estar en la capacidad de suplir o integrarse con tokens basados en software. g. Validación de equipos de plataformas Windows mediante la comprobación de sistema operativo, firewall de Windows, antivirus para obtener acceso mediante VPN SSL. h. Soporte nativo para al menos HTTP, FTP, SMB/CIFS, VNC, SSH, RDP y Telnet. i. Deberá poder verificar la presencia de antivirus (propio y/o de terceros) y de un firewall personal (propio y/o de terceros) en la máquina que establece la comunicación VPN SSL. j. Deberá tener soporte al concepto de registros favoritos (bookmarks) para cuando el usuario se registre dentro de la VPN SSL k. Debe ser posible definir distintos portales SSL que servirán como interfaz gráfica a los usuarios de VPN SSL luego de ser autenticados por la herramienta. Dichos portales deben poder asignarse de acuerdo con el grupo de pertenencia de dichos usuarios. l. Los portales personalizados deberán soportar al menos la definición de:	

	a. Widgets a mostrar b. Aplicaciones nativas permitidas. Al menos: HTTP, CIFS/SMB, FTP, VNC c. Soporte para Escritorio Virtual d. Política de verificación de la estación de trabajo e. La VPN SSL integrada debe soportar la funcionalidad de Escritorio Virtual, entendiéndose como un entorno de trabajo seguro que previene contra ciertos ataques además de evitar la divulgación de información. f. Se deberán configurar las características de VPN SSL e IPSEC que la unidad indique durante la fase de implementación y soporte a los equipos.	
9. Autenticación	El dispositivo deberá manejar los siguientes tipos de autenticación: a. Autenticación basada en contraseña y en doble factor de autenticación (certificado, correo, SMS y tokens). b. Capacidad de integrarse con Servidores de Autenticación: RADIUS, LDAP, TACACS+, POP3, SSO y RSA ACE. c. Soporte de tokens basados en software para dispositivos IOS o Android y hardware integrados a la solución de NGFW. d. Capacidad incluida, al integrarse con Microsoft Windows Active Directory debe autenticar transparentemente usuarios sin requerir username o password. Esto es aprovechar las credenciales del dominio de Windows bajo un concepto "Single-Sign-On". e. Se deberán configurar las características de autenticación que la unidad indique durante la fase de implementación y soporte a los equipos.	
10. Manejo de tráfico y calidad de servicio.	a. El equipo debe soportar traffic shaper basado en fuente (dirección IP, usuarios locales y grupos), destino (dirección IP, FQDN, URL o categoría), servicio (General, acceso web, acceso a archivos, servicios de correo y red, autenticación, acceso remoto, tunneling, VoIP, mensajería y otras aplicaciones, web proxy), aplicación, categoría de aplicaciones, categoría de URLs. b. El equipo debe permitir la configuración de reglas de prioridad de tráfico por dirección fuente, grupo de usuarios, dirección destino, numero de protocolo y aplicaciones basadas en nube. c. Capacidad de poder asignar parámetros de traffic shapping sobre reglas de firewall d. Capacidad de poder asignar parámetros de traffic shaping diferenciadas para el tráfico en distintos sentidos de una misma sesión e. Capacidad de definir parámetros de traffic shaping que apliquen para cada dirección IP en forma independiente, en contraste con la aplicación de las mismas para la regla en general. f. Capacidad de poder definir ancho de banda garantizado en KiloBytes por segundo	

	g. Capacidad de poder definir límite de ancho de banda (ancho de banda máximo) en KiloBytes por segundo h. EL proveedor deberá configurar las características de manejo de tráfico y calidad del servicio que la unidad indique durante la fase de implementación y soporte a los equipos.	
11. Antimalware	a. Debe ser capaz de analizar, establecer control de acceso y detener ataques y hacer antivirus en tiempo real en al menos los siguientes protocolos: HTTP, SMTP, IMAP, POP3, FTP, NNTP, HTTPS, IMAPS, POP3S, SMTPS y FTPS. b. Debe mitigar las siguientes amenazas: Virus, gusanos, troyanos, ransomware, scareware, spyware, adware, botnets, entre otros. c. El módulo de antimalware debe haber sido desarrollado por el mismo fabricante de la solución de firewall, así como las firmas deberán ser de su propiedad y no por medio de licenciamiento o concesiones de un tercero, esto con el fin de garantizar la idoneidad de la protección, así como los tiempos de respuesta del soporte de la misma. d. El Antivirus deberá poder configurarse de forma que los archivos que pasan sean totalmente capturados y analizados, permitiendo hacer análisis sobre archivos que tengan varios niveles de compresión. e. El Antivirus deberá integrarse de forma nativa con el sandbox, de tal manera que envíen muestras de archivos a dicho dispositivo para su análisis. f. El antivirus debe permitir las siguientes opciones de inspección: amenazas en ejecutables Windows que se encuentran embebidas en un adjunto de correo electrónico y protección para malware de dispositivos móviles. g. Antivirus en tiempo real, integrado a la plataforma de seguridad “appliance”. Sin necesidad de instalar un servidor o appliance externo, licenciamiento de un producto externo o software adicional para realizar la categorización del contenido. h. El Antivirus integrado debe soportar la capacidad de inspeccionar y detectar virus en tráfico IPv6. i. El antivirus deberá escanear tráfico de compartición de archivos: CIFS, SMB y SAMBA. j. La solución debe soportar la integración con soluciones de Sandbox. k. La solución deberá integrarse de forma nativa con una solución de Sandbox local, sin la necesidad de desarrollos adicionales o licencias adicionales. l. La solución debe incluir mecanismos para detectar y detener conexiones a redes Botnet y servidores C&C m. Durante la fase de implementación el proveedor deberá configurar las características que la Entidad requiera, realizando las demostraciones (simulando ataques de malware) de funcionamiento y protección del antimalware, con el fin de garantizar que las características implementadas cumplen su	

	función de forma estricta. Se deben realizar los ajustes que sean necesarios en caso de detectar alguna anomalía.	
12. Filtrado WEB	a. La solución debe permitir filtrado de contenido web, filtrado de URLs y servicio de filtrado web basado en firmas desarrolladas por laboratorio de investigación y desarrollo propio del fabricante. b. Facilidad para incorporar control de sitios a los cuales naveguen los usuarios, mediante categorías. Por flexibilidad, el filtro de URLs debe tener por lo menos 75 categorías y por lo menos 47 millones de sitios web en la base de datos. c. Debe poder categorizar contenido Web requerido mediante IPv6. d. La solución debe permitir realizar el filtrado de contenido, tanto realizando reconstrucción de toda la sesión como realizando inspección paquete a paquete sin realizar reconstrucción de la comunicación. e. Capacidad de filtrado de scripts en páginas web (JAVA/Active X). f. La solución de Filtrado de Contenido debe soportar la característica de “Safe Search” o “Búsqueda Segura” para prevenir imágenes y sitios web con contenido explícito en los resultados de búsqueda. Esto debe ser soportado para los siguientes motores de busqueda: Google, Yahoo y Bing. g. Debe ser posible exceptuar la inspección de HTTPS por categoría. h. El filtrado de contenido web debe permitir la definición de palabras, frases, patrones, wildcards y expresiones regulares Perl para prevenir acceso a páginas con material cuestionable. i. El sistema de filtrado de URLs debe incluir la capacidad de definir cuotas de navegación basadas en categoría, grupo de categoría o clasificación. j. La solución debe poder aplicar distintos perfiles de navegación de acuerdo con el usuario que se esté autenticando. Estos perfiles deben poder ser aplicados a usuarios o grupos de usuarios. k. El filtrado debe ser sobre tráfico HTTP y HTTPS. l. El proveedor debe implementar las características de cifrado que la Entidad establezca durante el proceso de implementación verificando su correcto funcionamiento y realizando los ajustes que sean requeridos.	
	a. Los sistemas de detección y prevención de intrusos deben poder implementarse tanto en línea como fuera de línea. En línea, el tráfico a ser inspeccionado pasará a través del equipo. Fuera de	

13. Protección contra intrusos (IPS)	línea, el equipo recibirá el tráfico a inspeccionar desde un switch con un puerto configurado en span o mirror. b. Deberá ser posible seleccionar el sistema operativo, protocolo, severidad y objetivo para la configuración de perfiles IPS. c. Deberá ser posible definir políticas de detección y prevención de intrusiones para tráfico IPv6 a través de sensores. d. El IPS debe tener la posibilidad de tomar las siguientes acciones: permitir, monitorear, bloquear, resetear la sesión, guardar copia de los paquetes que coincidan con las firmas, hacer cuarentena con base en dirección IP del atacante y tiempo basado en días, horas o minutos. e. El sistema de protección de intrusos debe utilizar decodificadores de protocolo para identificar patrones de tráfico anormal que no reúnan los requerimientos de protocolo y estándares. f. Capacidad de detección de más de 4000 ataques. g. Capacidad de actualización automática de firmas IPS mediante tecnología de tipo “Push” (permitir recibir las actualizaciones cuando los centros de actualización envíen notificaciones sin programación previa), adicional a tecnologías tipo “pull” (Consultar los centros de actualización por versiones nuevas) h. El sistema de detección y prevención de intrusos deberá estar integrado a la plataforma de seguridad “appliance”. Sin necesidad de instalar un servidor o appliance externo, La interfaz de administración del sistema de detección y prevención de intrusos deberá de estar perfectamente integrada a la interfaz de administración del dispositivo de seguridad appliance, sin necesidad de integrar otro tipo de consola para poder administrar este servicio. Esta deberá permitir la protección de este servicio por política de control de acceso. i. El sistema de detección y prevención de intrusos deberá soportar captar ataques por variaciones de protocolo y además por firmas de ataques conocidos (signature based / Rate base), realizando actualización automática de dichas firmas. j. El sistema de detección y prevención de intrusos deberá mitigar los efectos de los ataques de negación de servicios. k. Se deben configurar los siguientes métodos de notificación: o Alarmas mostradas en la consola de administración de los appliance. o Alertas vía correo electrónico.	

	o Debe tener la capacidad de cuarentena, es decir prohibir el tráfico subsiguiente a la detección de un posible ataque. Esta cuarentena debe poder definirse al menos para el tráfico proveniente del atacante o para el tráfico del atacante al atacado. o La capacidad de cuarentena debe ofrecer la posibilidad de definir el tiempo en que se bloqueará el tráfico. También podrá definirse el bloqueo de forma "indefinida", hasta que un administrador tome una acción al respecto. o Integración con sistema de monitoreo y correlación de eventos FortiSIEM para que éste notifique y el servicio de SOC pueda realizar SOC escalamientos requeridos.	
14. Control de Aplicaciones	a. Debe basarse en categorías que permitan seleccionar grupos de firmas basados en un tipo de categoría. b. La solución debe soportar la capacidad de identificar la aplicación que origina cierto tráfico a partir de la inspección del mismo. c. La identificación de la aplicación debe ser independiente del puerto y protocolo hacia el cual esté direccionado dicho tráfico. d. El listado de aplicaciones debe actualizarse periódicamente. e. Para aplicaciones identificadas deben poder definirse al menos las siguientes opciones: permitir, bloquear, hacer traffic shapping, registrar en log, ver firmas y bloquear acceso a una aplicación por un periodo de tiempo específico basado en días, horas y minutos. f. Para aplicaciones no identificadas (desconocidas) deben poder definirse al menos las siguientes opciones: permitir, bloquear, registrar en log. g. Para aplicaciones de tipo P2P debe poder definirse adicionalmente políticas de traffic shaping. h. Debe ser posible inspeccionar aplicaciones tipo Cloud como YouTube, Dropbox, Baidu, Amazon entre otras entregando información como login de usuarios, transferencia de archivos y videos visualizados. i. El proveedor deberá configurar las características de control de aplicaciones que la entidad establezca durante la fase de implementación, realizando las comprobaciones de funcionalidad y realizando los ajustes necesarios.	

15. Inspección de Contenido SSL/SSH	a. La solución debe soportar inspeccionar tráfico que esté siendo encriptado mediante SSL al menos para los siguientes protocolos: HTTP, IMAP, SMTP, POP3. b. Debe ser posible definir perfiles de inspección SSL donde sea posible definir los protocolos a inspeccionar y el certificado usado, estos perfiles deben poder ser escogidos una vez se defina la política de seguridad. c. Debe ser posible definir si la inspección se realiza desde múltiples clientes conectando a servidores (es decir usuarios que navegan a servicios externos con SSL) o protegiendo un servidor interno de la entidad. d. La inspección deberá realizarse: mediante la técnica conocida como Hombre en el Medio (MITM – Man In The Middle) para una inspección completa o solo inspeccionando el certificado sin necesidad de hacer full inspection. e. Para el caso de URL Filtering, debe ser posible configurar excepciones de inspección de HTTPS. Dichas excepciones evitan que el tráfico sea inspeccionado para los sitios configurados. Las excepciones deben poder determinarse al menos por Categoría de Filtrado. f. El equipo debe ser capaz de analizar contenido cifrado (SSL o SSH) para las funcionalidades de Filtrado de URLs, Control de Aplicaciones, Prevención de Fuga de Información, Antivirus e IPS g. Debe ser posible inspeccionar tráfico SSH y funcionalidades como Exec, Port-Fortward o X11. h. El proveedor deberá configurar las características de inspección SSL/SSH que la entidad establezca durante la fase de implementación, realizando las comprobaciones de funcionalidad y realizando los ajustes necesarios.	
16. Alta Disponibilidad	a. El dispositivo deberá soportar Alta Disponibilidad transparente, es decir, sin pérdida de conexiones en caso de que un nodo falle tanto para IPV4 como para IPV6 b. Se debe configurar Alta Disponibilidad en modo Activo-Activo de forma automática sin requerir hacer políticas de enrutamiento basado en orígenes y destino para poder hacer la distribución del tráfico. c. Se deben definir al menos dos interfaces para sincronía d. La alta disponibilidad debe configurarse de forma que el uso de Multicast no sea necesario en la red e. Se deben definir interfaces de gestión independientes para cada miembro en un clúster.	

	f. Durante la fase de implementación se deben realizar las pruebas que demuestren que la correcta configuración de la alta disponibilidad.	
17. Visibilidad	a. La solución debe estar en la capacidad de visualizar el tráfico de usuario, aplicaciones, navegación y niveles de riesgo en tiempo real, esto deberá ser sobre la misma plataforma sin necesidad de software o licenciamiento adicional. b. El equipo debe permitir la visualización de la topología física y lógica, con el fin de obtener mayor información de los dispositivos y conexiones. c. El equipo debe entregar las siguientes consolas para reunir los siguientes objetivos: o Políticas: Permite monitoreo de actividad de políticas, con el fin de discernir cuales políticas no se usan y pueden ser borradas. o Interfaces: Permite realizar monitoreo actual e histórico de ancho de banda por interfaz. o Países: Filtrado de trafico de acuerdo a países fuente y destino. o Traffic shaping: Permite monitoreo de traffic shappers configurados. o Mapa de amenazas: Permite monitorear riesgos provenientes de varias ubicaciones internacionales llegando a una ubicación específica. o Autenticaciones fallidas: Permite determinar si el NGFW presenta un ataque de fuerza bruta, asi como: acceso no autorizado a interfaz por telnet, SSH, HTTP y HTTPS, fallas para hacer una consulta por SNMP, intentos fallidos para establecer conexión de una VPN IPSec Dial-up, conexiones de VPNs IPSec Sitio a Sitio y conexiones de VPNs SSL. d. Menú tipo dropdown para navegar por la información. e. Mostrar los origenes del tráfico o usuarios que lo generan. f. Mostrar las aplicaciones y su categorización según riesgo. g. Visibilidad de las amenazas o incidentes que han ocurriedo en la red h. En la información de fuentes, aplicaciones, navegación debe ser posible con un doble-click filtrar la información para ser más específica la búsqueda. i. Se deben ver aplicaciones, sitios, amenazas por cada usuario.	

	j. Se debe ver el tiempo de navegación por cada sitio o categoría de sitios. k. De las aplicaciones Cloud que permitan compartir archivos como Dropbox debe ser posible ver que archivos fueron subidos y descargados por los usuarios.	
18. Características de Administración	a. Interfaz gráfica de usuario (GUI), vía Web por HTTP y HTTPS para hacer administración de las políticas de seguridad y que forme parte de la arquitectura nativa de la solución para administrar la solución localmente. Por seguridad la interfaz debe soportar SSL sobre HTTP (HTTPS) b. Interfaz basada en línea de comando (CLI) para administración de la solución. c. Puerto de consola dedicado para administración. Este puerto debe estar etiquetado e identificado para tal efecto. d. Comunicación cifrada y autenticada con usuario y contraseña, tanto como para la interfaz gráfica de usuario como la consola de administración de línea de comandos (SSH) e. El administrador del sistema podrá tener las opciones incluidas de autenticarse vía usuario/contraseña y vía certificados digitales. f. Los administradores podrán tener asignado un perfil de administración que permita delimitar las funciones del equipo que pueden gerenciar y afectar. g. El equipo ofrecerá la flexibilidad para especificar que Los administradores puedan estar restringidos a conectarse desde ciertas direcciones IP cuando se utilice SSH, Telnet, http o HTTPS. h. El equipo deberá poder administrarse en su totalidad (incluyendo funciones de seguridad, ruteo y bitácoras) desde cualquier equipo conectado a Internet que tenga un browser (Internet Explorer, Mozilla, Firefox) instalado sin necesidad de instalación de ningún software adicional. i. Soporte de al menos 3 servidores syslog para poder enviar bitácoras a servidores de SYSLOG remotos j. Soporte de Control de Acceso basado en roles, con capacidad de crear al menos 6 perfiles para administración y monitoreo del Firewall. k. Monitoreo de comportamiento del appliance mediante SNMP v3 y v3, el dispositivo deberá ser capaz de enviar traps de SNMP cuando ocurra un evento relevante para la correcta operación de la red.	

	l. Debe ser posible definir la dirección IP que se utilizará como origen para el tráfico iniciado desde el mismo dispositivo. Esto debe poder hacerse al menos para el tráfico de alertas, SNMP, Log y gestión. m. Permitir que el administrador de la plataforma pueda definir qué funcionalidades están disponibles o deshabilitadas para ser mostradas en la interfaz gráfica. n. Contar con herramientas gráficas para visualizar fácilmente las sesiones en el equipo, que permitan adicionarse por el administrador en la página inicial de la solución (dashboard), incluyendo por lo menos por defecto Top de sesiones por origen, Top de sesiones por destino, y Top de sesiones por aplicación.	
19. Virtualización	a. El dispositivo deberá poder virtualizar los servicios de seguridad mediante "Virtual Systems", "Virtual Firewalls" o "Virtual Domains" b. La instancia virtual debe soportar por lo menos Firewall, VPN, filtro de contenido web, IPS, control de aplicaciones, antimalware, con todas las funcionalidades requeridas en la sección correspondiente a cada característica del presente documento. c. Se debe incluir la licencia para al menos 10 (diez) instancias virtuales dentro de la solución a proveer, de los cuales se deberán configurar como mínimo dos acorde a los requerimientos de la entidad. d. Cada instancia virtual debe poder tener un administrador independiente e. La configuración de cada instancia virtual deberá poder estar aislada de manera lógica del resto de las instancias virtuales. f. Cada instancia virtual deberá poder estar en modo gateway o en modo transparente a la red g. Debe ser posible la definición y asignación de recursos de forma independiente para cada instancia virtual h. Debe ser posible definir distintos servidores de log (syslog) para cada instancia virtual. i. Debe ser posible definir y modificar los mensajes mostrados por el dispositivo de forma independiente para cada instancia virtual. j. Debe ser posible definir enlaces de comunicación entre los sistemas virtuales sin que el tráfico deba salir de la solución por medio de enlaces o conexiones virtuales, y estas conexiones	

	deben poder realizarse incluso entre instancias virtuales en modo NAT y en modo Transparente k. Se debe poder ver el consumo de CPU y memoria de cada instancia virtual. l. El proveedor deberá configurar las características de virtualización aquí descritas durante el proceso de implementación, de acuerdo con los requerimientos de la Entidad.	
20. Certificados de fabricante	a. El Proveedor debe ser canal (partner) certificado con el máximo nivel del fabricante de los equipos ofertados y estar en capacidad técnica de configurar, mantener y dar soporte técnico de los equipos. En consecuencia, el oferente deberá presentar la certificación que lo acredite como partner con el máximo nivel del fabricante. Este documento debe ser expedido por el fabricante de los equipos ofertados con fecha no mayor a 30 días dirigido a la Sociedad de Activos Especiales.	
21. Implementación	a. Los equipos deben ser configurados para soportar la operación de la Entidad, configurando el enrutamiento, interfaces de red, reglas de tráfico, políticas, controles de aplicaciones y navegación, controles de tráfico y demás configuraciones que la entidad defina para la implementación optima de los equipos y su interacción con los demás componentes de la infraestructura. Todas estas configuraciones se deben realizar tanto para IPv4 como para IPv6, garantizando el funcionamiento en modo dual-stack de la red de la Entidad. Para esto el proveedor debe prestar su asesoría como experto en los equipos adquiridos y en seguridad informática para que la Entidad implemente de forma óptima los equipos en todas sus funcionalidades en protocolo IPv4 e IPv6.	
22. Implementación y Puesta en Marcha	a. Levantamiento de información previo a la instalación de la solución de firewalls. Se debe realizar la instalación, configuración, actualización y puesta en marcha de la solución. b. Cualquiera de las características contenidas en este documento deberá ser configurada y puesta en operación durante la vigencia del contrato si la Entidad determina que debe implementarse. c. Presentar Plan de trabajo y cronograma de trabajo dentro de los quince (15) días siguientes a la suscripción del acta de inicio, para aprobación del supervisor y realizar los ajustes a que haya lugar.	

	d. Todas las funcionalidades y características ofrecidas deben incluir el correspondiente licenciamiento a perpetuidad. e. La implementación deberá comprender los siguientes puntos: • Diseño y planeación de cada una de las actividades minimizando la afectación del servicio. • Configuración y alistamiento de la plataforma a la última versión estable aprobada por el fabricante. • Implementación de la solución de acuerdo con las mejores prácticas de los fabricantes, teniendo en cuenta una arquitectura de red segura. • Pruebas de Servicio. • Puesta en Producción. • Estabilización de la plataforma. f. La instalación, configuración y puesta en marcha de los equipos debe incluir transferencia de conocimiento y capacitación necesaria para la administración de la totalidad de las funcionalidades del equipo entregado. La capacitación debe ser certificada directamente por el fabricante.	
23. Documentación	a. EL contratista deberá entregar a la entidad • Manuales del fabricante del producto propuesto. • Documentación, que registre el estado de configuración e implementación al momento de la recepción formal de la solución (Informe definitivo de la Implementación) • Diagramas y planos. • Documentos de garantía • Manuales de administración. • Manuales de operación. • Manuales de usuario. • Documentación de licenciamiento. • Catálogos de la herramienta ofrecida. b. Es obligatorio, para el cumplimiento del requisito habilitante, incluir en su propuesta el catálogo o documentación técnica del fabricante, en el cual se permita la comprobación de lo ofrecido, se debe diligenciar este anexo indicando el Número de folio.	

5.5 Requerimientos Firewall de aplicaciones y Balanceador de cargas

Se deberán ofrecer, configurar y poner en operación las funcionalidades que se detallan en la siguiente tabla

EQUIPOS OFRECIDOS:_____

CARACTERÍSTICA	REQUERIMIENTO TÉNICO	CUMPLIMIENTO (indicar capacidades o características si aplican)
1. Generalidades.	a. Se requiere una solución dedicada a la protección de aplicaciones WEB del tipo Web Application Firewall. Esta solución debe ser de tipo virtual appliance, donde la entidad suministrara la infraestructura para virtualizar dicho virtual appliance. b. La solución debe ser de la misma marca de los firewalls de nueva generación descritos en el punto anterior. c. Los equipos deben integrarse de forma nativa (fábrica) con el appliance virtual de monitoreo y correlación de eventos con el que cuenta la entidad (FortiSIEM). d. Debe configurarse eficientemente para proteger las Aplicaciones Web de la entidad de amenazas externas, con el rendimiento necesario para proteger otros portales web que la entidad publique sin requerir licenciamiento adicional. e. La solución debe permitir fácil y rápidamente implementar controles basado en políticas internas hacia los servidores web de la entidad. f. La solución debe poder restaurar los portales web de forma automática en caso de presentarse una modificación no autorizada. g. La plataforma propuesta debe identificar vulnerabilidades a un número ilimitado de aplicativos web de la entidad, sin requerir licenciamiento adicional. h. La solución deberá realizar balanceo de tráfico para garantizar disponibilidad de las aplicaciones web protegidas. Con las siguientes características: - Métodos de balanceo: Round robin, least conection i. La solución deberá contar con sus respectivas actualizaciones periódicas a nivel de firmas de seguridad durante el periodo contratado. j. La solución deberá ser totalmente compatible con IPv6.	

	k. La solución debe poderse implementar en modo proxy reverso, transparente o monitoreo. Sin embargo en conjunto con la entidad se definirá la mejor opción a nivel de configuración de seguridad. l. El fabricante deberá estar como recomendado por NSS Labs a nivel de Firewall de Aplicaciones Web. m. El equipo deberá tener la capacidad de integrarse de forma nativa con una solución de sandbox, sin requerir desarrollos adicionales. n. La plataforma es requerida por un periodo de 3 años en un esquema 7 x 24 ante fabricante.	
2. Desempeño Requerido	a. Throughput HTTP mínimo de 500 Mbps b. Virtual CPU de mínimo 8 cores c. Número de aplicaciones web a proteger y que deben entregarse aseguradas con el WAF: Ilimitado	
3. Protección de Aplicaciones Firewall de aplicaciones web	a. La solución deberá integrar firmas de amenazas y ataques conocidos y deberá proteger de ataques nuevos o de día cero actualizándose durante el tiempo de la garantía: - Cross-Site Scripting (XSS) - SQL Injection - Remote File Inclusion - Local File Inclusion - OS Commands - Troyanos y virus - Exploits - Información Sensible del servidor - Fugas de Información - Firmas personalizadas b. Con esto la herramienta debe ser capaz de proteger de las siguientes amenazas: - Adobe Flash Binary (AMF) protocol Attack. - Botnet - Browser Exploit Against SSL /TLS - Clickjacking - Cookie Tampering - Credit Card Theft - Cross Site request forgery - Cross site Scripting - DoS - HTTP Header Overflow - Local File Inclusion	

	- Malicious Robots - Man in the Middle - Remote File Inclusion - Server information leakage - SQL Injection - Malformed XML	
4. Protección contra Web Defacement	Con el fin de garantizar la reputación de la Entidad y la integridad de las aplicaciones web, la solución deberá contar con un módulo de anti-defacement el cual permita monitorear las aplicaciones, alertar y de ser necesario restaurar en caso de modificaciones no autorizadas de las aplicaciones web protegidas, la solución deberá poder monitorear la integridad de los archivos por medio de FTP, SSH o SMB, por lo tanto no se acepta soluciones que requieran la instalación de agentes, los cuales generan carga adicional a los servidores.	
5. Análisis de vulnerabilidades	El oferente deberá garantizar una solución para realizar análisis de vulnerabilidades sobre las aplicaciones web protegidas, de tal forma que se identifiquen vulnerabilidades existentes en los aplicativos web de la entidad de forma ilimitada, sin requerir licenciamiento adicional.	
6. Protección DoS	La solución deberá contar con un módulo de prevención contra ataques de denegación de servicio en http y https de tal forma que proteja a las aplicaciones web contra este tipo de ataques, dicho módulo deberá permitir como mínimo las siguientes acciones: - Alertar. - Denegar. - Bloquear por un Periodo de Tiempo.	
7. Auto aprendizaje de las aplicaciones web	a. La solución debe contar con la funcionalidad de auto aprendizaje de aplicaciones, la cual permita crear una línea base del comportamiento de la aplicación para creación de diferentes políticas de protección de un número ilimitado de aplicativos web. b. La solución debe contar con métodos de detección de ataques que no estén basados únicamente en firmas, sino que incluyan motores de Inteligencia Artificial (IA) y de Machine Learning (ML) basados en modelos matemáticos y probabilísticos que permitan recolectar, aprender, probar y regenerar los datos que deben ser aceptados en los parámetros del sitio web protegido. c. La solución debe aprender de forma automática los métodos usados en los sitios web protegidos.	

	d. La solución debe contar con dos motores de Inteligencia Artificial (IA) y Machine Learning (ML) independientes, uno para la detección de anomalías en los parámetros protegidos y el otro que identifique ataques en los mismos	
8. Antimalware	e. La solución deberá contar con un módulo de escaneo AntiMalware para hacer una revisión de los archivos que sean posteados o subidos a las aplicaciones web, permitiendo ejecutar las siguientes acciones: - Detección y bloqueo de malware conocido a nivel de los archivos que se cargan a las aplicaciones web. - Permitir la integración nativa con una plataforma del tipo Sandbox, para la detección y bloqueo de malware de Dia cero. f. La solución deberá contar con protección de ataques basados en la localización geográfica del atacante.	
9. Prevención de Fuga de Información.	La solución deberá contar con un módulo para la prevención de fuga de información, el cual permita crear reglas personalizadas basadas en patrones, este módulo deberá ser completamente funcional sin requerir licencias adicionales o integraciones con plataformas de terceros.	
10. Autenticación.	a. La solución deberá permitir la creación de reglas de autenticación, dichas reglas de autenticación deberán permitir: - Autenticación por medio de LDAP o Radius. - Autenticación de doble factor por medio de Token. - (SSO) Single Sign-On para portales tales como OWA, SharePoint, etc.	
11. Prevención Fuerza Bruta.	La solución deberá contar con un módulo de prevención de ataques de fuerza bruta contra los portales de autenticación de la entidad y los aplicativos web, el cual permita bloquear por un periodo de tiempo al atacante, dicho periodo de tiempo deberá poder ser parametrizado por la entidad	
11. Validación del Protocolo HTTP.	a. La solución deberá tener la capacidad de validar el protocolo HTTP, haciendo una revisión como mínimo de los siguientes parámetros: - Hostname. - Versión Http. - Método del Request. - Tamaño del Request. - Tamaño del Contenido. - Tamaño del Body.	

	- Tamaño del Header. - Número de Cookies en el request. - Número de Parámetros en la URL.	
12. Administración y Gestión de la Plataforma	a. Gestión vía HTTPS y CLI. b. Deberá contar con API por medio del método RESTful sobre HTTPS. c. La solución deberá contar con dashboards, que muestren como mínimo información en tiempo real del tráfico, Historia de Ataques, sesiones por política e información del sistema. d. La solución debe soportar ambientes multitenant, donde sea posible dividir la administración y aplicar políticas de WAF para ambiente en producción, preproducción, pruebas y desarrollo o las que decida la entidad.	
13. Instalación, configuración y puesta en operación	a. La solución deberá ser instalada y configurada en protocolo IPv4 e IPv6, permitiendo a la Entidad decidir cuales configuraciones se realizarán en cada protocolo o en caso de terminado, permitiendo a la entidad realizar la conversión de IPv4 a IPv6 de forma transparente para la aplicación y los usuarios. b. El proveedor deberá realizar todas las configuraciones de las características relacionadas en este documento que la Entidad considere durante la fase de implementación y durante el periodo de soporte. c. La instalación, configuración y puesta en marcha de los equipos debe incluir transferencia de conocimiento y capacitación necesaria para la administración de la totalidad de las funcionalidades del equipo entregado. La capacitación debe ser certificada directamente por el fabricante.	

6. MANTENIMIENTO PREVENTIVO Y CORRECTIVO

- El proveedor deberá realizar cómo mínimo 2 (dos) visitas de mantenimiento preventivo por cada año de soporte y garantía de la solución, realizando las actualizaciones de firmware y software (incluido software de gestión) necesarias, realizando las verificaciones del estado general de la plataforma, realizando los afinamientos que se puedan requerir, generado recomendaciones de acuerdo con las mejores prácticas del fabricante de la solución, implementando los requerimientos que la Entidad establezca para la operación adecuada de los mismos en la infraestructura de la Entidad. Para cada mantenimiento preventivo el proveedor deberá

destinar en sitio cómo mínimo 8 horas al ingeniero certificado en la solución para realizar las tareas mencionadas, independientes al tiempo que tome la actualización de firmware o del software.
Si, derivado de la aplicación de una nueva versión del software para alguna solución surge una nueva funcionalidad o mejora de una existente, el proveedor deberá informar a la Entidad y realizar la transferencia de conocimiento respectiva para que los administradores de la solución la gestionen, realizando el acompañamiento respectivo a la implementación en la Entidad.
Luego de finalizado cada mantenimiento, el proveedor deberá entregar la documentación de todas las actividades realizadas, con soportes gráficos que muestren los estados iniciales y finales del componente, las mejoras introducidas, los afinamientos realizados y sus resultadosl.

- El proveedor deberá realizar los mantenimientos correctivos que se requieran para cualquier componente de hardware o software entregado como parte las soluciones requeridas por la Entidad. Estos mantenimientos incluyen cambio de partes o componentes completos, los componentes deben ser nuevos, no remanufacturados y originales del fabricante de la solución.
  En caso de mantenimiento correctivo: Al finalizar cada visita correctiva y el proponente deberá entregar un informe de servicio en el que constará el resumen de las actividades realizadas (actualización, soporte y mantenimiento), problemas presentados, soluciones utilizadas y recomendaciones, así como las evidencias de estas actividades. De igual forma quedará constancia en la misma acta o informe de servicio si hubo cambio de software y/o en alguna configuración. Dicho informe deberá ser entregado durante los 5 días hábiles siguientes a la terminación de las tareas de mantenimiento.
  Si, derivado un mantenimiento correctivo para alguna solución, surge una nueva funcionalidad o mejora de una existente, el proveedor deberá informar a la Entidad y realizar la transferencia de conocimiento respectiva para que los administradores de la solución la gestionen, realizando el acompañamiento respectivo a la implementación en la Entidad.

7. SOPORTE TÉCNICO

El proveedor deberá prestar soporte técnico especializado durante la vigencia del contrato, de acuerdo con el equipo de trabajo mínimo requerido en el presente documento, para cada componente entregado. El servicio de soporte debe incluir atención de incidentes y consultas sobre la operación y administración de cualquiera de las soluciones entregadas a través de llamadas telefónicas, correo electrónico, sesiones remotas y atención en sitio en horario Hábil y No Hábil (7x24x365). La entidad indicará la modalidad de atención requerida, de acuerdo con la naturaleza del requerimiento y a la criticidad de este.

7.1 Procedimiento de reporte de casos de soporte

Durante la última semana de la fase de implementación, configuración y migración se deberá suministrar la siguiente información:

a. Nivel de escalamiento, indicando:
   1) Nivel de escalamiento, por ejemplo: primer, segundo, tercer, etc.
   2) Rol responsable del escalamiento, por ejemplo: mesa de ayuda, coordinador de servicio, líder de servicio, etc.
   3) Datos de contacto del responsable del rol:
   - Nombre completo (nombre(s) y apellido(s)) del responsable.
   - Dirección de correo electrónico.
   - Número (s) de teléfono.

b. Para el reporte de los casos de soporte:
   1) Si se tiene habilitada una plataforma web, suministrar la URL del Help Desk y las credenciales asignadas a la SAE, junto con un manual de operación que describa la entrada al sistema; la forma de colocar una incidencia, anexar documentos, hacerle seguimiento y aceptar o rechazar su solución.
   2) Direcciones de correo electrónico de contacto.
   3) Números telefónicos fijos y celulares.
   4) Nombres de los ingenieros de soporte.

La SAE abrirá los casos de soporte en primera instancia en el Help Desk del contratista vía web, en caso de estar habilitada; en segunda instancia, vía telefónica o email. El tiempo de atención para aplicación de los ANS empezará a contar desde el momento en que se produzca la solicitud y constituirán evidencia de ello: la fecha y hora de la generación del número de tiquete del Help Desk; o la fecha y la hora de la llamada; o la fecha y la hora del envío del email.

8 ACUERDOS DE NIVELES DE SERVICIOS

El proveedor deberá contar con un esquema de soporte técnico con atención de requerimientos e incidentes en modalidad 7x24, con los siguientes acuerdos de niveles de servicio:

NIVEL DE CRITICIDAD	DESCRIPCIÓN	TIEMPO MÁXIMO DE ATENCIÓN	TIEMPO MÁXIMO DE SOLUCIÓN	DISPONIBILIDAD DE ATENCIÓN	MODALIDAD DE ATENCION
Nivel 3 – Criticidad baja	Refiere incidentes o solicitudes de soporte técnico que no afectan la disponibilidad de los servicios que	4 horas	24 horas	5x8 (Next bussines Day)	Remoto o presencial de acuerdo con

NIVEL DE CRITICIDAD	DESCRIPCIÓN	TIEMPO MÁXIMO DE ATENCIÓN	TIEMPO MÁXIMO DE SOLUCIÓN	DISPONIBILIDAD DE ATENCIÓN	MODALIDAD DE ATENCION
	presta cualquiera de los componentes entregados.				requerimiento de la Entidad
Nivel 2 – Criticidad media	Refiere incidentes que afectan la disponibilidad de alguno de los servicios que presta cualquiera de los componentes entregados.	2 horas	4 horas	5x8	Remoto o presencial de acuerdo con requerimiento de la Entidad
Nivel 1 – Criticidad Alta	Incidentes que afectan por completo los servicios que presta cualquiera de los componentes entregados o fallas que puedan generar afectación por completo en cualquier momento.	30 minutos	2 horas	7x24	Remoto o presencial de acuerdo con requerimiento de la Entidad
	Incidentes que involucren cambio de partes de hardware pero que no afecten la operación del componente afectado.	1 hora	Next Bussiness Day	7x24	Presencial

9 EQUIPO DE TRABAJO MÍNIMO REQUERIDO

El proveedor debe garantizar la disponibilidad y dedicación del recurso humano necesarios para cumplir con la prestación del servicio, los cuales estarán bajo su cuenta y riesgo, entendiéndose que no se genera relación laboral con la Entidad, por ende, no existirá pago de prestaciones sociales ni de ningún tipo de costos distintos al valor acordado, por parte de la SAE.

Para garantizar la ejecución de las actividades requeridas en este documento, se deberá disponer del siguiente personal:

PROFESIONAL REQUERIDO CON SU PERFIL Y EXPERIENCIA					
Rol a desempeñar	**Formación Académica**		**Experiencia General**	**Experiencia Específica**	
	Pregrado	**Certificaciones o postgrado**		**Tiempo Como/En**	**Número mínimo de Contratos o proyectos**
Ingeniero coordinador de implementación	Ingeniero de: sistemas o electrónico o de comunicaciones o Telemático o de redes.	Debe contar con certificación en la plataforma de hiperconvergencia	Mínima de cuatro (4) años	Cuatro (4) años de experiencia como: Ingeniero implementador o coordinador en proyectos informáticos relacionados con el objeto y alcance del contrato, como mínimo con experiencia certificada en la solución hiperconvergente y los equipos de seguridad.	2
Ingeniero de implementación hiperconvergente	Ingenieros de: sistemas o electrónico o de comunicaciones o Telemático o de redes.	Debe contar con certificación en la plataforma de hiperconvergencia entregada	Mínima de tres (3) años	Tres (3) años de experiencia como: Ingeniero implementador o de soporte o de operación, sobre la plataforma hiperconvergente entregada.	1
Ingenieros de implementación de equipos de seguridad	Ingenieros de: sistemas o electrónico o de comunicaciones o Telemático o de redes.	Debe contar con certificación en la plataforma de firewalls UTM en el nivel avanzado del fabricante (integración de componentes de seguridad Firewall UTM y Firewall de aplicaciones)	Mínima de tres (3) años	Tres (3) años de experiencia como: Ingeniero implementador o de soporte o de operación, en los equipos de seguridad Firewall UTM y Firewall de aplicaciones entregados	1
Ingenieros de implementación de equipos de red	Ingenieros de: sistemas o electrónico o de comunicaciones o Telemático o de redes.	Debe contar con certificación en la plataforma de swicthes de core entregados.	Mínima de tres (3) años	Tres (3) años de experiencia como: Ingeniero implementador o de soporte o de operación, sobre la plataforma swicthes de core entregados.	1

La tabla anterior establece el equipo mínimo requerido para la ejecución de las tareas contempladas en este documento, sin embargo, el proveedor deberá proporcionar el

recurso humano que estime necesario para cumplir con los tiempos y alcance establecidos en el proceso de contratación.